ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits SAP
Numéro de Référence	43741309/23
Date de Publication	13 Septembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Product-SAP BusinessObjects Suite (Installer) versions 420 et 430
- S4 HANA ABAP (Manage checkbook apps) versions 102, 103, 104, 105, 106 et 107
- S4CORE (Manage Purchase Contracts App) versions 102, 103, 104, 105, 106 et 107
- SAP Business Client versions 6.5, 7.0 et 7.70
- SAP Business Objects Business Intelligence Platform (CMC) versions 420 et 430
- SAP BusinessObjects Business Intelligence Platform (Promotion Management) versions 420 et 430
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML inter-face) versions 420
- SAP BusinessObjects Business Intelligence Platform (versions Management System) versions 430
- SAP NetWeaver (Guided Procedures) versions 7.50
- SAP NetWeaver AS ABAP (applications based on Unified Rendering) versions SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 702 et SAP_BASIS 731
- SAP NetWeaver AS ABAP, SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KER-NEL 7.22, KERNEL 8.04, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KER-NEL64UC 7.53, KERNEL64UC 8.04, KERNEL64NUC 7.22 et KERNEL64NUC 7.22EXT
- SAP NetWeaver Process Integration versions 7.50
- SAP PowerDesignerClient versions 16.7

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- SAP Quotation Management Insurance (FS-QUO) versions 400, 510, 700 et 800
- SAP S/4HANA (Create Single Payment application) versions 100, 101, 102, 103, 104, 105, 106, 107 et 108
- SAP S/4HANA (Manage Catalog Items and Cross-Catalog search) versions S4CORE 103, S4CORE 104, S4CORE 105 et S4CORE 106
- SAP Web Dispatcher versions 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89
- SAPContent Server versions 6.50, 7.53, 7.54
- SAPExtended Application Services and Runtime (XSA) versions SAP_EXTENDED_APP_SERVICES 1, , XS_ADVANCED_RUNTIME 1.00
- SAPHANA Database versions 2.0
- SAPHost Agent versions 722
- SAPSSOEXT versions 17
- SAPUI5 versions SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756 et UI_700 200

Identificateurs externes

- CVE-2023-40622 , CVE-2022-41272 , CVE-2023-25616 , CVE-2023-40309 , CVE-2023-42472 , CVE-2023-40308 , CVE-2023-40621 , CVE-2023-40623 , CVE-2023-40306 , CVE-2021-41184 , CVE-2021-41183 , CVE-2021-41182 , CVE-2023-24998 , CVE-2023-40624 , CVE-2023-40625 , CVE-2023-37489 , CVE-2023-41367 , CVE-2023-41369 , CVE-2023-41368

Bilan de la vulnérabilité

SAP annonce la disponibilité d'une mise à jour de sécurité corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de porter atteinte à la confidentialité de données, de contourner la politique de sécurité, d'exécuter du code arbitraire à distance et de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité SAP du 12 Septembre 2023**.**

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance
- Déni de service

Annexe

Bulletin de sécurité SAP 12 Septembre 2023**:**

- https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=1&d=2023-09-13